The Future of Unmanned Aviation in the U.S. Economy: Safety and Privacy Considerations

Before

The United States Senate Committee on Commerce, Science, and Transportation

January 15, 2014
Good afternoon Chairman Rockefeller, Ranking Member Thune and Members of the Committee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU), its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, about the privacy and free speech implications of the domestic use of drones by the government and the private sector.

I. Introduction

Unmanned aircraft carrying cameras raise the prospect of a significant new avenue for the surveillance of American life. Many Americans are familiar with these aircraft, commonly called drones, because of their use overseas in places like Afghanistan, Pakistan and Yemen. But drones are coming to America. Under 2012 legislation, the Federal Aviation Administration is required to “develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system.”¹ This legislation has dramatically accelerated the deployment of drones and pushed this issue to the forefront.

At the same time, drone technology is quickly becoming cheaper and more powerful while our privacy laws have not kept up with the technology. Aerial surveillance from manned aircraft has been with us for decades. One of the first aircraft the Wright brothers built was a surveillance aircraft, and it was sold to the U.S. Army. But manned aircraft are expensive to purchase, operate and maintain, and this expense has always imposed a natural limit on the government’s aerial surveillance capability. Now that surveillance can be carried out by unmanned aircraft, this natural limit is eroding. The prospect of cheap, small, portable flying surveillance platforms threatens to eradicate existing practical limits on aerial monitoring and allow for pervasive surveillance. Our current privacy laws are not strong enough to ensure that this new technology will be used responsibly and consistently with constitutional protections against unchecked government scrutiny embodied in the Fourth Amendment.

At the same time, many prospective uses of drone aircraft—newsgathering, search and rescue, fighting wildfires—are beneficial and some are constitutionally protected. We must respect the long held First Amendment rights of freedom of speech and of the press in any regulation of the private use of drones. This statement explores the variety of issues surrounding the measures that Congress can take to safeguard Americans’ constitutional values in the coming world of drones.

II. The Technology

There are hundreds of different types of Unmanned Aerial Vehicles (UAVs), as drones are formally known. They can be as large as commercial aircraft or as small as hummingbirds,

¹ FAA Modernization and Reform Act of 2012, P.L. 112-95, §332, 126 Stat.11, 73.
and include human remotely guided aircraft as well as autonomous, self-guided vehicles. They include:

- **Large fixed-wing aircraft.** The largest drones currently in use, such as the Israeli-made Eitan, are about the size of a Boeing 737 jetliner. The Eitan’s wingspan is 86 feet, and it can stay aloft for 20 hours and reach an altitude of 40,000 feet. In Pakistan and Afghanistan, the U.S. military and CIA deploy Predators and Reapers armed with surveillance capability as well as missiles capable of destroying a moving vehicle from thousands of feet in the air.

- **Small fixed-wing aircraft.** Smaller fixed-wing aircraft are the current favorite for domestic deployment. The Houston police department, for example, recently tested the ScanEagle, made by Boeing subsidiary Insitu. The ScanEagle is 5 ½ feet long with a wingspan of 10 feet, and it can climb to 19,500 feet and stay aloft for more than 24 hours.

- **Backpack craft.** Another class of craft is designed to be carried and operated by a single person. The hand-launched AeroVironment Raven, for example, weighs 4 pounds, has a wingspan of 4.5 feet and a length of 3 feet, can fly up to 14,000 feet and stay aloft for up to 110 minutes. Individual hobbyists have also built a number of drones in this size range.

- **Hummingbirds.** A tiny drone called the Nano Hummingbird was developed for the Pentagon’s Defense Advanced Research Projects Agency (DARPA) by AeroVironment. Intended for stealth surveillance, it can fly up to 11 miles per hour and can hover, fly sideways, backwards and forwards, for about 8 minutes. It has a wingspan of 6.5 inches and weighs only 19 grams—less than a single AA battery.

---


5 Insitu, ScanEagle brochure, online at [http://www.insitu.com/systems/scaneagle](http://www.insitu.com/systems/scaneagle).


• **Blimps.** Some blimps are envisioned as high-altitude craft, up to 300 feet in diameter, that would compete with satellites, while others would be low-altitude craft that would allow the police to monitor the streets. Supporters say they are more cost-effective than other craft due to their ability to stay aloft for extended periods. 8

### III. Drone Capabilities—Today and in the Future

The aircraft themselves are steadily improving and, as with so many technologies, that is almost certain to continue. They are becoming smaller. The military and law enforcement are keenly interested in developing small drones, which have the advantages of being versatile, relatively cheap to buy and maintain, and in some cases so small and quiet that they will escape notice. 9 They are also becoming cheaper. The amazing continual decreases in the prices of electronics that have become normal in our time all but guarantee that the surveillance technologies attached to drones will become less expensive and yet more powerful—and with mass production, the aircraft that carry those electronics will become inexpensive enough for a police department or commercial entity to fill the skies over a town with them.

Drones are also becoming smarter. Artificial intelligence advances will likely help drones carry out a variety of missions. Korean researchers, for example, are working to teach robots how to hide from and sneak upon a subject. 10 Recently, Amazon CEO Jeff Bezos revealed the company’s plans to create an automated drone delivery service. 11 Drones will also have better staying power, with a greater ability to stay aloft for longer periods of time. Mechanisms for increasing time aloft could include solar power, or the use of blimps or gliders. 12

Although the primary users of drones so far has been the military and CIA, even on overseas battlefields their most frequent use is surveillance. Some of the larger drones can be fitted with weapons or other heavy payloads, but all of them can carry cameras and other

---


imaging technologies that have developed amazing capabilities in recent years and are likely to become even more capable in the near future.

Except for possibly the very lightest craft, drones can carry the full range of advanced surveillance technologies that have been developed—and are likely to be developed. Drones will certainly have capacity to gather more and better information than the unaided human eye through the use of high powered zoom lens, infrared and ultraviolet imaging and perhaps even technology that allows for see-through imaging.\textsuperscript{13}

This capacity will extend not just to collection of information but also analytics as this field seeks to apply artificial intelligence techniques not just to collect but also to “watch” video. One of the most significant uses would be to continually track individuals or vehicles as they move about, using face recognition or other bodily characteristics.\textsuperscript{14} It might also be used to identify particular movement patterns as “suspicious,” or to identify and flag changes in routines, buildings or grounds.\textsuperscript{15} Computers performing these tasks have a distinct advantage over human observers, because as one observer summed it up, “machines do not blink or forget. They are tireless assistants.”\textsuperscript{16}

The PBS series NOVA, “Rise of the Drones,” recently aired a segment detailing the capabilities of a powerful aerial surveillance system known as ARGUS-IS. This system, which includes a super-high, 1.8 gigapixel resolution camera mounted on a drone, demonstrates many of these capacities. The system is capable of high-resolution monitoring and recording of an entire city. To witness a demonstration of this capacity, please see: http://www.youtube.com/watch?v=13BahrdkMU8

\textbf{IV. Drone Use: Harms and Benefits}

Drones are a powerful new technology which may have deep and lasting impacts on American life. On one hand, they raise the prospect of a significant new avenue for surveillance. The prospect of routine aerial surveillance is on the near horizon and would profoundly change the character of public life in the United States. It could, if unchecked by appropriate legal protections, bring our country a large step closer to a “surveillance society” in which every move is monitored, tracked, recorded, and scrutinized by the authorities.


At the same time, there are potential positive uses of drones, such as drone-based photography for applications like newsgathering, art and government accountability. Much as the inclusion of digital cameras into smartphones has revolutionized things like citizen journalism and the ability of Americans to document police abuse, the availability of cheap, unobtrusive drones may allow improvements to civil liberties and other areas of American life. Given this reality, what are the dangers and what are the benefits of drone use?

a. **Harms**

The reasons for concern reach across a number of different dimensions:

- **Chilling effects.** What would be the effect on our public spaces, and our society as a whole, if everyone felt the keen eye of the government or corporate surveillance whenever they ventured outdoors? Psychologists have repeatedly found that people who are being observed tend to behave differently, and make different decisions, than when they are not being watched. This effect is so great that a recent study found that “merely hanging up posters of staring human eyes is enough to significantly change people’s behavior.”


- **Voyeurism.** The widespread use of video surveillance has revealed how susceptible this technology can be to individual abuse, including voyeurism. In 2004, a couple making love on a dark nighttime rooftop balcony, where they had every reason to expect they enjoyed privacy, were filmed for nearly four minutes by a New York police helicopter using night vision. This is the kind of abuse that could become commonplace if drone technology enters widespread use. (Rather than apologize, NYPD officials flatly denied that this filming constituted an abuse, telling a television reporter, “this is what police in helicopters are supposed to do, check out people to make sure no one is … doing anything illegal”).

- **Mission creep.** Even where drones are being envisioned for positive uses, such as search and rescue, fighting wildfires, and in dangerous tactical police operations, they are likely to be quickly embraced by law enforcement around the nation for other, more controversial purposes. The Department of Homeland Security (DHS) uses drone surveillance as
part of its border security mission. However, over the last three years there has also been an eight-fold increase in the ‘lending’ of those drones to federal, state, and local police for other law enforcement.\(^{19}\) Further, as drones become more commonplace in the private sector, there will be an increased appetite to access that footage for law enforcement and other government use. The ACLU has written extensively about this problem of government and private sector surveillance partnerships in other contexts.\(^{20}\)

- **Abuse.** The individuals operating surveillance systems bring to the job all their existing prejudices and biases. In Great Britain, camera operators have been found to focus disproportionately on people of color. According to a sociological study of how the systems were operated, “Black people were between one-and-a-half and two-and-a-half times more likely to be surveilled than one would expect from their presence in the population.”\(^{21}\) In addition, sometimes bad policies are set at the top, and an entire law enforcement agency is turned toward abusive ends. During the labor, civil rights, and anti-Vietnam war movements of the 20th century, the FBI and other security agencies engaged in systematic illegal behavior against those challenging the status quo. And once again today we are seeing an upsurge in spying against peaceful political protesters across America.\(^{22}\)

- **Tracking.** The Justice Department currently claims the authority to monitor Americans’ comings and goings using cell phone and GPS tracking devices—under uncertain legal standards. Fleets of drones, interconnected and augmented with analytics software, could enable the mass tracking of vehicles and pedestrians around a wide area.

- **Automated enforcement.** Drones are part of a trend toward automated law enforcement, in which cameras and other technologies are used to mete out justice with little or no human intervention. This trend raises a variety of concerns, such as the fact that computers lack the judgment to evaluate the circumstances surrounding a supposed violation fairly, and may be susceptible to bugs and other software errors, or simply are not programmed to encapsulate the state of the law as passed by legislatures fairly and properly.\(^{23}\)


\(^{22}\) See ACLU “Spyfiles” web site at [www.aclu.org/spyfiles](http://www.aclu.org/spyfiles).

b. **Benefits**

In turn, while recognizing and seeking to curb the damaging effects of drones, we must also safeguard the areas where drones can bring positive developments to American life:

- **Newsgathering.** A journalist in Turkey used to a drone to record demonstrations in a public park and another in South Africa used a drone to capture “aerial shots of intense activity around the hospital” where Nelson Mandela was being treated.\(^{24}\) Formal news media organizations may also use drones to cover more news events, at lower costs, through what is being called drone-based-journalism. A Drone Journalism Lab has already been created with the support of the University of Nebraska-Lincoln.\(^{25}\)

- **Filmmaking.** Drones can give filmmakers new vantage points to film or inexpensive methods to gather footage. For example, a drone helped one filmmaker capture the Gettysburg battlefield for a Civil War documentary\(^{26}\) and another take beautiful video of an anonymous skateboarder in Prague.\(^{27}\) Similarly, a local bank used footage filmed from a drone to help with security and employee training.\(^{28}\)

- **Government Accountability.** During the Occupy Wall Street protests in 2011, activist-blogger Tim Pool modified the $300 Parrot AR Drone to create “Occucopter”, which provided live feeds of the Occupy protests that were broadcast on UStream.\(^{29}\) The right of citizens to record the police is a critical check and balance. It creates an independent record of what took place in a particular incident, free from accusations of bias, lying or faulty memory. Visual evidence of police activity has often been crucial in investigating and reigning in police misconduct.\(^{30}\)

We can achieve meaningful privacy protections while still enjoying the benefits of drone technology. Many of the clearest benefits of drone use are either protected by the First Amendment or do not need to involve the collection of personal information while the greatest abuses can be stemmed by strong statutory, judicial and institutional controls.

---

\(^{24}\) Mickey H. Osterreicher, Use of Unmanned Aerial Vehicles in Newsgathering, The Sky’s the Limit – Or is it?,” Media Law Resources Center.


\(^{26}\) Osterreicher.


\(^{28}\) Osterreicher.


\(^{30}\) Jay Stanley, “You Have Every Right to Photograph That Cop,” ACLU, Sept. 7, 2011, online at https://www.aclu.org/free-speech/you-have-every-right-photograph-cop
V. Existing Legal Protections

In order to consider how to best strike this balance, we must first review the applicable law. The following two sections address the current legal regimes impacting drone use and provide our recommendations for improving privacy and safeguarding free speech when regulating drone technology.

a. Fourth Amendment

As described above, many of the most significant potential harms from unchecked use of drones come from the government. Unfortunately, we won’t know for many years whether the constitutional protections enshrined in the Fourth Amendment will be able to provide meaningful protections against abuse. There are no Supreme Court cases ruling on drones although the court has allowed some warrantless aerial surveillance from manned aircraft. In the 1986 decision California v. Ciraolo, the Supreme Court focused on whether an individual has a privacy interest in being free from aerial surveillance of his backyard. In spite of the defendant’s high fence the court stated there was not a privacy intrusion because “[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed.”

Similarly in Dow Chemical Co. v. United States, the Supreme Court held that a precision aerial mapping camera taking photographs of a chemical plant was simply conventional photography and “not so revealing of intimate details as to raise constitutional concerns.” In Florida v. Riley, the court authorized a search where a police officer flew over a greenhouse and spotted marijuana through a broken pane in a greenhouse roof. Unsurprisingly, many law enforcement agencies, including the FBI, read this case law as granting them almost unfettered authority to collect information using drones.

On the other hand, in a recent decision in U.S. v. Jones, a concurrence joined by five justices held that ubiquitous, long term tracking of an individual raised constitutional concerns. Five justices in that case agreed that “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.” While this case involved tracking through a GPS device, the underlying reasoning could well apply to drone technology. As drone technology becomes more prevalent, it is easy to imagine a future where cataloguing an individual’s movement on the public streets is a reality. A

robust interpretation of Jones is critical to protecting American’s privacy and modernizing the Fourth Amendment. But whatever the Supreme Court eventually decides, it is clear the technology is moving far more rapidly than Fourth Amendment jurisprudence.

b. First Amendment

In addition to the Fourth Amendment and other privacy rights, several federal courts have relied on free speech analysis in holding that taking photographs of things that are plainly visible from public spaces is a constitutional right protected by the First Amendment. This right adheres regardless of whether the photographer is a member of the traditional media, and we believe that the growth of citizen journalists and maturation of photographic technologies require strict First Amendment protections for all photographers, be they reporters, concerned citizens, protesters or artists. Furthermore, the technology used to gather this information – be it a high resolution handheld camera or a drone – does not and should not reduce these protections. As a result, any restrictions on private drone photography must comport with the requirements of the First Amendment.

As a general matter, the government is not forbidden from regulating drone use, including drone photography, so long as drone restrictions are not aimed at expressive activity. With respect to newsgathering, and although courts should generally tread lightly to avoid First Amendment problems, journalists of all stripes enjoy no special immunity from laws of general applicability like antitrust, copyright or the rules of the air.

Because laws on expressive activity must be carefully tailored to important government interests, any restrictions on drones’ ability to access or record publicly-viewable matter should only be enacted in response to well understood and articulated privacy harms and narrowly crafted to the greatest extent possible toward those important public purposes. Additionally, if any regulation targets only certain speakers or viewpoints, it will be subject to the highest level of constitutional scrutiny and will likely be deemed unconstitutional under the First Amendment. In other words, if only specific types of photography are allowed, such as for scientific research

---

35 See Iacobucci v. Boulter, 193 F.3d 14, 25 (1st Cir. 1999) (holding that plaintiff’s activities involved “the exercise of his First Amendment rights” when he took video of government official following a public meeting and was subsequently arrested); Fordyce v. City of Seattle, 55 F.3d 436 (9th Cir. 1995) (sustaining cause of action against police officer for assaulting photographer filming political demonstration under First Amendment); Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000) (find a First Amendment right, subject to reasonable time, manner and place restrictions, to photograph or videotape police conduct.

36 See, e.g., Glik v. Cunniffe, 655 F.3d 78, 82 (1st Cir. 2011) (holding that “[i]t is firmly established that the First Amendment's aegis extends further than the text's proscription on laws ‘abridging the freedom of speech, or of the press,’ and encompasses a range of conduct related to the gathering and dissemination of information” (collecting cases); Pomykacz v. Borough of W. Wildwood, 438 F. Supp. 2d 504, 513 (D.N.J. 2006) (holding that citizen activism including monitoring and photographing of police officers is “clearly protected by the First Amendment”).

or police search and rescue missions, but others like commercial photojournalism are barred, this will trigger strict scrutiny by the courts.\(^{38}\)

In sum, Congress may enact reasonable, neutral rules for the use of drones that are connected to particular privacy harms but may not favor particular types of drone photography over others.

c. Federal Aviation Administration (FAA) regulation

At least one agency, the FAA, has already begun to craft such neutral rules. The FAA Modernization and Reform Act of 2012 requires the FAA to integrate drones into the national airspace by the end of 2015. As the FAA has recently acknowledged, privacy needs to be part of that process.\(^{39}\) The FAA has determined that the best avenue to develop privacy protection is by integrating their development with the agency’s existing mandate to choose six test sites, each for five years, for drone research.\(^{40}\) These test sites are “defined geographic area[s] where research and development are conducted.”\(^{41}\)

Accordingly, the FAA has created the following privacy requirements for each test site operator:

1. Maintain and update a publicly available privacy policy which governs all drone operators;
2. Create a mechanism to receive public comment on its policy;
3. Conduct an annual audit of test site operations and assure that all operators are compliant;
4. Comply with all applicable privacy law; and
5. Require all drone operators to have a written plan for retention and use of data collected.\(^{42}\)

The agency’s goal with these regulations is not only to govern test site operators but also provide an “opportunity for development and demonstration by the test site operators and users of policies and operating approaches that would address both drone operator mission needs and related individual privacy concerns. The lessons learned and best practices established at the test


\(^{40}\) “Not later than 180 days after the date of enactment of this Act, the Administrator shall establish a program to integrate unmanned aircraft systems into the national airspace system at 6 test ranges. The program shall terminate 5 years after the date of enactment of this Act.” FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332(c)(1), 126 Stat 11 (2012). The six entities chosen as test sites are the University of Alaska, State of Nevada, New York’s Griffiss International Airport, North Dakota Department of Commerce, Texas A&M University – Corpus Christi, and Virginia Polytechnic Institute and State University (Virginia Tech).

\(^{41}\) Id. at § 331(7).

\(^{42}\) 78 Fed. Reg. 68360.
sites may be applied more generally to protect privacy in UAS operations throughout the NAS. [National Airspace]”

d. **Tort and Peeping Tom Laws**

In addition to the protections of the Fourth Amendment and rules promulgated by the FAA, state and federal statutory laws and common law also protect individual privacy rights and apply to the use of drones.

Modern tort law recognizes four torts – the legal term for injury to a plaintiff for which they are entitled relief – relating to privacy. The most relevant for a discussion of drones is for harms relating to “intrusion upon seclusion” which has been adopted by all but two states. It is described by the Second Restatement of Torts as “one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns.” This invasion must be “highly offensive to a reasonable person.” The Restatement states that this tort applies to “use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires.” Any invasion under this standard must be “outrageous to a person of ordinary sensibilities” and objectively offensive. As a general matter, claims are more likely to be successful if the intrusion is into the home and less so when it takes place in public.

Two other connected tort claims that an individual monitored by a drone flight could claim would be trespass – accessing private property – and nuisance – interfering with the use and enjoyment of an individual’s land. While the common law rule that a property owner owns their land “to the heavens” has largely eroded over the last century, these two torts may still apply to drone flights. According to the Second Restatement on Torts, trespass includes “flight by aircraft in the airspace above the land of another is a trespass if, but only if, (a) it enters into the immediate reaches of the airspace next to the land, and (b) it interferes substantially with the other's use and enjoyment of his land.” The Restatement suggests immediate reaches of airspace includes those under 500 feet. That is airspace where at least some drone flight is likely

---

43 Unmanned Aircraft Systems Comprehensive Plan, Pg 7.
44 The full list is:
1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.
45 Alissa Dolan and Richard Thompson II. *U.S. Congressional Research Service. Integration of Drones into Domestic Airspace: Selected Legal Issues* (7-5700; April 4, 2013), online at: [http://www.fas.org/sgp/crs/natsec/R42940.pdf](http://www.fas.org/sgp/crs/natsec/R42940.pdf) North Dakota and Wyoming are the two states that have not adopted the tort.
46 REST 2d TORTS § 652B
48 CRS Report, Integration of Drones into Domestic Airspace.
49 REST 2d TORTS § 159.
to take place. Nuisance claims are similar. They are also based on interference with an owner’s enjoyment of their land but do not require actual occupation of the owner’s airspace.\textsuperscript{50} Nuisance and some intrusions on seclusion claims (most notably those that do not involve a physical invasion) may in some cases implicate other First Amendment protected activities.

State and federal laws also criminalize a variety of privacy invasions, typically referred to as peeping tom laws. For example under federal law there is a one year criminal penalty for capturing an image of a “private area of an individual” without their consent in a circumstance where the individual has a reasonable expectation of privacy.\textsuperscript{51} This law only applies on federal property. States laws vary in definitions and details but tend to have a similar focus, criminalizing viewing or capturing an image of someone who is undressed or partially dressed when they have a reasonable expectation of privacy.\textsuperscript{52} These state laws sometimes contain exceptions for when the viewing or filming conducted by law enforcement.

e. State Drone Legislation

Finally, state legislatures are already responding to the need to safeguard against drone surveillance. According to the National Conference of State Legislatures, “in 2013, 43 states introduced 118 bills and resolutions concerning drone issues. So far, 16 bills have been enacted in 13 states and 14 resolutions have been adopted in 10 states.”\textsuperscript{53} These piece of legislation are too many and varied to summarize here but the vast majority of these bills are focused squarely on privacy issues associated with drone use.

VI. ACLU Recommendations

Government and private sector drone use operate under different legal frameworks. The government currently operates with few restrictions and drone use represents significant potential for immediate harm. In the private sector, harms are also significant but may be buffered by additional legal protections and important countervailing First Amendment interests. Given that reality, the ACLU recommends two different responses. Congress should place immediate, robust restriction on the government use of drones, especially as part of criminal investigations, in order to prevent mass aerial surveillance. On the private sector side, it should take a more deliberate path – one that recognizes the serious privacy dangers, limits sharing with government, explores existing legal protections and actively monitors privacy rules promulgated by the FAA.

a. Government surveillance

\textsuperscript{50} REST 2d TORTS § 821D.
\textsuperscript{51} 18 U.S.C. § 1801.
\textsuperscript{52} A list of state laws compiled by the National District Attorneys Association can be found here: http://www.ndaa.org/pdf/voyeurism_statutes_mar_09.pdf
Drones can be an extremely powerful surveillance tool, and their use by law enforcement must be subject to strict limitations, as should all government power. In addition to the courts, Congress also has a duty to uphold the constitution and should enact statutory protections that bolster those found in the Fourth Amendment.

At a minimum, Congress should enact the following core measures to ensure that this happens:

- **Usage restrictions.** Drones should be subject to strict regulation to ensure that their use does not eviscerate the privacy that Americans have traditionally enjoyed and rightly expect. Innocent Americans should not have to worry that police will scrutinize their activities with drones. To this end, the use of drones should be prohibited for indiscriminate mass surveillance, for example, or for spying based on First Amendment-protected activities. In general, drones should not be deployed by the government except:

  o where there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific instance of criminal wrongdoing or, if the drone will intrude upon non-public spaces, then the government must first obtain a warrant based on probable cause; or

  o where required for a geographically confined, time-limited emergency situation in which particular individuals’ lives are at risk, such as a fire, hostage crisis, or person lost in the wilderness; or

  o for reasonable non-law enforcement purposes by non-law enforcement agencies, where privacy will not be substantially affected, such as geological inspections or environmental surveys, and where the surveillance will not be used for secondary law enforcement purposes or for any purpose other than the stated purpose.

- **Image retention restrictions.** Images of identifiable individuals captured by aerial surveillance technologies should not be retained or shared unless there is reasonable suspicion that the images contain evidence of criminal activity or are relevant to an ongoing investigation or pending criminal trial.

- **Public notice.** The policies and procedures for the use of aerial surveillance technologies should be explicit and written, and should be subject to public review and comment. While it is legitimate for the police to keep the details of particular investigations confidential, policy decisions regarding overall deployment policies—including the privacy trade-offs they may entail—are a public matter that should be openly discussed.
- **Democratic control.** Deployment and policy decisions surrounding drones should be democratically decided based on open information—not made on the fly by police departments simply by virtue of federal grants or other autonomous purchasing decisions or departmental policy fiat.

- **Auditing and effectiveness tracking.** Investments in drones should only be made with a clear, systematic examination of the costs and benefits involved. And if aerial surveillance technology is deployed, independent audits should be put in place to track the use of drones by government, so that citizens and other watchdogs can tell generally how and how often they are being used, whether the original rationale for their deployment is met, whether they represent a worthwhile public expenditure, and whether they are being used for improper or expanded purposes.

- **Ban on weaponization.** Weapons developed on the battlefield in Iraq and Afghanistan have no place inside the U.S. The national consensus on this issue is reflected by the fact that the Heritage Foundation and the International Association of Chiefs of Police join us in supporting sharp limits on weaponized drones.\(^{54}\)

Ultimately, this powerful new technology should only be used by the government if subject to an equally powerful framework that regulates its use in order to avoid abuse and invasions of privacy.

b. **Commercial Drone Use**

Use of drones by the private sector also presents serious privacy risks, though those risks must be counterbalanced by real and important First Amendment values. In addition, unlike in the case of government drones, existing legal frameworks may provide some measure of protection against these dangers. As Congress and the FAA consider this issue, we would urge policy makers to consider several general propositions about the application of the First Amendment to drones, and particularly to aerial photography using drones:

- As with all photography, policy makers must take care not to regulate the actual expression—in this case, the photographs—and must focus on regulating or punishing improper uses of those photographs (extortion, for instance, or infringements on the right of publicity). In no case should lawmakers draft laws that single out newsgathering using

---

drones for special restrictions over and above those applicable to non-newsgathering applications.

- The constitutional right to photograph anything visible from a public vantage point—including, and in particular, government activity—must be protected. Policy makers should not distinguish between amateur or professional photographers in doing so.

- Other restrictions on photographs and other information taken or collected using drones should be proportionate to the privacy threat represented. Existing and constitutional laws punishing the inappropriate use of photographs should be explored and evaluated before Congress or federal regulators issue new laws or regulations that single out drone photography for special treatment.

- Congress and federal regulators should resist efforts to expand already overbroad anti-paparazzi or anti-whistleblower laws to drone photography, including so-called constructive invasion of privacy torts and “ag gag” laws that make unauthorized photography of businesses involving agricultural or animal products subject to special restrictions.

Even within these necessary restrictions, there are still some areas where it is already clear that legislation will be necessary. One immediate area of concern that will require Congressional action is the sharing of information between the private sector and police for the purposes of criminal law enforcement.

History has demonstrated that information held by the private sector frequently ends up in the hands of government, often in ways that policy makers didn’t anticipate and legal protections don’t address. For example, while the Privacy Act of 1974 is aimed at regulating and safeguarding personal information held by the federal government, federal agencies now circumvent those protections by turning to private data brokers, whose database contains personal information on millions of Americans. Those entities are not regulated by the Privacy Act and routinely provide information that is both inaccurate and inaccessible to its subjects. Given the real and pressing problems we have already described with government drone use, law enforcement must not be able to avoid legal controls by accessing private drone footage.

We also applaud the FAA for beginning the process of exploring privacy controls and its continuing commitment to using the Fair Information Practice Principles (FIPPs) as an appropriate framework making those determinations. The FIPPs are longstanding best practices in data collection and management. In addition to safeguarding First Amendment rights, here are

some of the issues policy makers will likely need to address as they consider application of the FIPPS in this new area:

- **Transparency:** In many cases drone operators will have to create and make publicly available a data collection policy that explains the data that is being collected and includes a catalog of any violations of the policy. In addition, the FAA should explore whether technological solutions exist that would allow the public to track the location of drone during flights.

- **Individual Participation:** Community involvement is critical in any drone regulation. Residents might be given an opportunity to opt their property out of surveillance. If personally identifiable information (PII) collected, the public should have a method to redress privacy violations.

- **Purpose Specification and Use Limitations:** Drones should be flown only pursuant to specific, articulated purposes which are made public. Use of captured data should be limited by these purpose specifications and unnecessarily collected PII should be deleted or obscured except for auditing purposes.

- **Data Quality and Integrity:** Affected residents should have the ability to correct inaccuracies in the PII aggregated by the use of drones and that the information collected has not been altered or destroyed in an unauthorized manner.

- **Security:** Data collection statements and test plans should detail the security used for communication between ground stations and drones. All communications should be encrypted when audiovisual content is being transmitted.

- **Accountability and Auditing:** In large scale or commercial drone operations, employees should be familiar with their privacy policy and trained in compliance. The FAA should also play an ongoing rule in this auditing and compliance.

The specter of routine aerial surveillance in American life is on the near horizon — a development that would profoundly change the character of public life in the United States. We need a system of rules that complies with the First and Fourth Amendment and ensures that Americans can enjoy the benefits of drone technology without bringing our country a large step closer to a “surveillance society” in which every move is monitored, tracked, recorded, and scrutinized by the authorities.

---

56 Note that, as described in section V. (c), some of these measures have already been adopted by the FAA for the operators of drone test sites.

57 For example the popular Google Streetview has the capacity to blur the faces of individuals and license plates caught by Google’s cameras. See Google Streetview Privacy Policy at: [http://www.google.com/intl/en_us/maps/about/behind-the-scenes/streetview/privacy/#streetview](http://www.google.com/intl/en_us/maps/about/behind-the-scenes/streetview/privacy/#streetview)